数理解析研究所講究録
932巻 1995年 118-124

On the notions of randomness

Mariko Yasugi
Faculty of Science, Kyoto Sangyo University
Kita-ku, Kyoto 603, Japan
e-mail: yasugi@cc.kyoto-su.ac.jp.

Abstract

A speculation on von Mises' type notion of randomness will be presented. Ideas proposed by Doob, Church and Loveland on this theme will first be outlined, and then a principle of selecting subsequences will be proposed.

Introduction

The notion of randomness with coin-tossing as a typical model has attracted many mathematicians, including mathematical logicians. As is known, von Mises attempted to give a mathematical formulation to it in terms of the concept *Kollektiv* and developed the theory of *Kollektiv*. We will not go into the theory of *Kollektiv*, but will explain briefly some of the succeeding works by Doob, Church and Loveland.

In order to make the story simple, we will consider an infinite sequence of two symbols, h and t, meaning *head* and *tail*. That is, the universe of discourse is $\Omega^{\mathbf{N}}$, where Ω is the set $\{h, t\}$ and N is the set of positive integers. The question is, how to characterise *random* ones among the sequences in $\Omega^{\mathbf{N}}$.

What the predecessors above agree on the notion of randomness is the following.

Let $\{a_i\}$be a sequence from $\Omega^{\mathbf{N}}$. $\{a_i\}$is said to be *random* if it satisfies the conditions (1) and (2) below. Let $\sigma(a_i)$denote 1 if a_i is h, and 0 if it is t.

(1) $\Sigma_{i=1}^{n}\sigma(a_i)/n$ converges to a real number p as n tends to ∞, where $0 < p < 1$.

(2) Let $\{a_{n_j}\}$ be any *admissible* subsequence of $\{a_i\}$. Then $\Sigma_{k=1}^{j}\sigma(a_{n_k})/j$ converges to p as j tends to ∞.

Everybody would agree on (1).

A subsequence is *admissible* if it is chosen according to *some principle of selection.* It is this *principle* that has to be speculated on and, hopefully, settled. It would probably be agreed that

(*) selection of an element a_i may depend only on information with regards to some finitely many elements of the sequence excepting a_i.

Let us set (*) as the requirement for a selection function of admissible subsequences.

We expect that there be a principle, which I temporarily call **P**, such that, given a sequence $\{a_i\}$, it is determined by **P** whether to select a_i or not. **P** is thus expected to contain some (local) information on $\{a_i\}$. It is obvious that **P** ought to regulate the selection so that not all the subsequences be selected.

Doob in [1] sets a scheme called a *system*, representing a principle *P*.

A *system* is a sequence of functions

$$\tau_1, \tau_2(a_1), \tau_3(a_1, a_2), \cdots, \tau_i(a_1, \cdots, a_{i-1}), \cdots$$

where the values of the functions are *yes* or *no.*

τ_1 is a constant, meaning that a_1 be chosen or not by default. $\tau_i(a_1, \cdots, a_{i-1})$ decides whether to select a_i or not according to information on $< a_1, \cdots, a_{i-1} >$. Betting in gambling is a typical model of this system.

In [1], it is demonstrated that "a successful system is impossible"; that is, "betting in accordance with it leaves the player in the same position as if he had bet on the result of each trial."

This version of the selection rule **P** has the property that

(A) given a $\{a_i\}$, whether a_i be selected or not depends only on information with regards to $< a_1, \cdots, a_{i-1} >$.

It is not clear, however, what kind of a function be allowed for a *system.*

Church in [2] proposed *recursive* functions as candidates of such. Let me explain his idea with my phrases.

Let ϕ be any recursive function, and let $\{b_n\}$ be a sequence of positive integers defined as follows.

$$b_1 := 1; b_{n+1} := 2b_n + \sigma(a_n)$$

It is an enumeration of finite sequences $< \sigma(a_1), \cdots, \sigma(a_{m-1}) >$. b_n is computed primitive recursively in terms of the basic function $2x + y$ by substituting b_{n-1} for x and $\sigma(a_n)$ for y. We can thus express the sequence $\{b_n\}$ with a function β as follows.

$$b_1 = \beta(1, <>) := 1$$

$$b_{n+1} = \beta(n+1, < a_1, \cdots, a_n >) := 2\beta(n, < a_1, \cdots, a_{n-1} >) + \sigma(a_n)$$

b_n thus depends only on $< a_1, \cdots, a_{n-1} >$.

Next, define $c_n := \phi(b_n)$ and $C := \{n | c_n = 1\}$. Under the assumption that C be an infinite set, arrange its elements in the increasing order: $\{n_j\}_j$. This scheme can be a candidate for a selection rule as required in (2) which satisfies (A). For, it is obvious that c_n is computed with information given by $< a_1, \cdots, a_{n-1} >$. We can thus write c_n as $c_n = \psi(n, < a_1, \cdots, a_{n-1} >)$. ψ is recursive in $\{a_i\}$. $\{n_j\}_j$ is then determined as follows.

$$n_1 := min(m; \psi(m, < a_1, \cdots, a_{m-1} >) = 1)$$

$$n_{j+1} := min(m; m \geq n_j + 1 \wedge \psi(m, < a_1, \cdots, a_{m-1} >) = 1)$$

n_j as a function of j is recursive in $\{a_i\}$, as the infinity of the set C is assumed.

Now, asked if a_i be chosen, one computes $\psi(i, < a_1, \cdots, a_{i-1} >)$ and see if the value be 0 or 1. So, $\psi(i, \_)$ can be adopted as the system $\{\tau_i\}$. That is, this selection scheme is in accord with Doob's *system*. Let us say $\{a_i\}$is *C-random* if it is random in this sense.

A recursive funtion produces values in a *regular* manner and hence one can expect that it does not destroy randomness as it selects a subsequence. Church then proves that there are many (in fact with power **c**) *C-random* sequences.

Much later than these predecessors, Loveland in [3] came up with another view on the selection principle. He explains an example of a situation in which a selction rule not satisfying the property (A) can be realistic. That is, selection of a_i may depend on information with regards to some $a_{k_1}, \cdots, a_{k_j}$, where the subscripts may be greater than i.

He gives a method how to construct a selection rule which does not violate the condition (*) but does not obey (A).

In the next section, I will give a mathematical formulation to this idea.

1 Church-Loveland-randomness

Given a sequence $\{a_i\}$, which is random in the sense of Church. Let ν be a *recursive re-enumeration* of positive integers. Its inverse, say μ is also recursive. $\{a_{\nu(l)}\}(=\{d_l\})$ will be a re-enumeration of $\{a_i\}$. (It can easily be seen that the condition (1) does not necessarily hold with $\{d_l\}$.)

We will define a function to determine a *system*, which realizes a selection principle, in a manner similar to ψ above.

Let $\{b'_n\}$ be a sequence of positive integers defined as follows.

$$b'_1 = \beta'(1, <>) := 1$$

$$b'_{n+1} = \beta'(n+1, < a_{\nu(1),\cdots,a_{\nu(n-1)}}>)$$
$$:= 2\beta'(n, < a_{\nu(1)}, \cdots, a_{\nu(n-1)} >) + \sigma(a_{\nu(n)})$$

Let ϕ be any recursive function. Then, define $c'_n := \phi(b'_n)$ and $C' := \{n|c'_n = 1\}$. Under the assumption that C' be an infinite set, arrange its elements in the increasing order: $\{n_j\}$. c'_n can be computed with information with regards to $< a_{\nu(1)}, \cdots, a_{\nu(l)} >$. We can thus write c'_n as $c'_n = \psi'(n, < a_{\nu(1)}, \cdots, a_{\nu(l)} >)$. c'_n is recursive in $\{a_l\}$, depending only on $< a_{\nu(1)}, \cdots, a_{\nu(l)} >$.

Put $q = q_i = \mu(i)$. That is, $a_i = a_{\nu(q)}$. We would like to decide whether to select a_i or not according to the scheme given by ψ'. That is, a_i will be chosen if and only if $c_q = 1$. The original sequence $\{a_i\}$will be said to be *L-C-random* if it satisfies (1) and (2) with the selection rule ψ' as above.

The idea is simple and natural. As a very special case of ν, we can take the identity function, and hence *C–L-random* sequences are *C-random.*

Loveland presents a construction method such that it produces a sequence $\{a_i\}$which is *C-random* but not *C-L-random.* This guarantees the significance of Loveland's generalization of the notion of randomness. The construction is an elaborate one relying on a diagonal method.

He also proves the existence of *C-L-random* sequences by the classical methods emplyoed by Doob and Church.

2 Beyond Recursive Selection

As was mentioned above, *recursive* selection for the condition (2) (whether it be *C-random* or *C-L-random*) is a safe way of selection, due to its regularity.

I am not sure, however, if it is sufficient. It is a matter of how one views *betting* decision.

Given information on $< a_1, \cdots, a_{i-1} >$, how would one decides whether or not to bet on a_i? In a way, this decision could be quite *random* (?!), for one can make decision quite capriciously. One can even toss a coin! In reality, one would like to *win* over a game, and hence would evaluate the preceding results and decide on a pre-set rule of judgement. Such a rule is usually recursive, as one has to make decision in a finite time interval. If one becomes desparate, however, one may toss a coin or rely on some omen. The selection procedure as such still does not depend on the information of a_i itself

Since Doob does not specify the selection rule, all these are admissible. Even then, mathematically, there are *random* sequences with power $\mathbf{c}$. It is now at our liberty what kind of selection rules (called $\mathbf{P}$ above) we admit. $\mathbf{P}$ can be expressed in terms of a scheme δ:

$$c_n := \delta(n, < \sigma(a_1), \sigma(a_2), \cdots, \sigma(a_{n-1}) >)$$

A most *regular* δ would be *recursive*, and a most *irregular* one would be *coin-tossing* or something of the sort.

In reality, one would rely on some kind of decidable criteria. For example, with 69 *heads* and 31 *tails*, one may feel that, since 69 is more than twice 31, the next tossing result would be *tail.* Being betrayed at the next stage, the player may judge that, for awhile, the lady luck is on the side of *head.* So, the player will bet on *head.*

Each of these judgements is decidable. The first one is to ask

(a) if $h_n > 2t_n$,

and the second one is to ask

(b) if $h_n > 2t_n$ and $\sigma(a_n) = 1$.

(h_n is the number of heads by n stages.) There is, however, no predetermined rule what kind of judgement be adapted at each stage. The player may suddenly getsa hunch that a_{n+1} be 1, and so the player bets on a_{n+1}.

In order that $\mathbf{P}$, the selection principle, cover all these possibilities of selection and yet be consistent in the sense that *almost all* sequences (from $\Omega^{\mathbf{N}}$) be random with repsect to $\mathbf{P}$, a sensible condition be that $\mathbf{P}$ be *recursive in a parameter.* Such a parameter is usually called an *oracle.* I thus propose the following.

Proposal *The selction principle* **P** *be represented in terms of functions which are recursive in an oracle.*

More explicitly, express **P** as follows.

Definition 2.1 *Let f be a number-theoretic function with a function parameter α. f is said to be recursive in the oracle α, if the follwoing it is defined by one of the following.*

$$f(x_1, \cdots, x_n) := c(c \quad \textit{is a constant.} \quad)$$

$$f(x_1, \cdots, x_n) := x_i(i = 1, \cdots, n)$$

$$f(x_1, \cdots, x_n) := \alpha(x_1, \cdots, x_n)$$

$$f(x_1, \cdots, x_n) := h(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$$

$$f(x) := x + 1$$

$$f(x, x_1, \cdots, x_n) := \quad \textit{if} \quad x = 0 \quad \textit{then} \quad h(x, x_1, \cdots, x_n)$$

$$\textit{else} \quad g(f(x-1, x_1, \cdots, x_n), x, x_1, \cdots, x_n)$$

$$\begin{gathered} f(x_1, \cdots, x_n) := \quad \textit{if} \quad g(x_1, \cdots, x_n, y) = 0 \\ \textit{then} \quad y \quad \textit{else} \quad f(x_1, \cdots, x_n, y+1) \end{gathered}$$

Here g and h are supposed to be recursive in α , *and have already been defined.*

(See [4] for details.)

Obviously, a recursive function is obtained as a special case of the definitions above. For (a) above, one can set as follows.

$$\alpha(n+1, < s_1, \cdots, s_n >) = 1 \quad \text{if and only if} \quad h_n > 2t_n$$

Here, s_i is $\sigma(a_i)$, and h_n is the number of h's (1's) among $a_1, \cdots, a_n$; similarly with t_n. For (b), α can be determied similarly. Notice that this is *not* determined uniformly in n, but is for this particular $n+1$. At another stage, say m, one may prefer to tossing another coin for decision, and gets t. Then, $\alpha(m, <\cdots>) = 0$, a constant.

The scheme as proposed above still fits in Doob's concept of *system*. Mathematical details are yet to be worked out.

References

[1] J.L. Doob, *Note on Probability*, Annals of Mathematics, vol.37(1936), 363-367

[2] A. Church, *On the concept of a random sequence*, Bulletin of AMS, vol.46(1940), 130-135

[3] D. Loveland, *A new interpretation of the von Mises' concept of random sequence*, Zeitschrift f. math.Logik und Grundl. d. Math.,Bd.12(1966).279-294

[4] M. Davis, R. Sigal and E. Weyuker, *Computability, Complexity, and Languages*, Academic Press, San Diego, 1994